

Anleitung zur Verschlüsselung & Entschlüsselung von E-Mail-Dateien im Deutschen Qualitätsbündnis Sepsis

Bei Rückfragen erreichen Sie uns unter info@cuviba.com oder +49 176 23933652

Zusammenfassung

Sie (Teilnehmer des Deutschen Qualitätsbündnisses Sepsis DQS) senden uns (cuviba) vertragsgemäß pseudonymisierte §21-Daten Ihrer Häuser. Der Kooperationsvertrag des DQS verpflichtet uns, Daten nur verschlüsselt auszutauschen. Wir verwenden daher ein PGP-Kryptographie-Verfahren mit öffentlichem und privatem Schlüssel.

Wenn Sie uns Daten senden, verschlüsseln Sie die Daten vor dem Versand mit unserem (cuviba) öffentlichen Schlüssel. Nur wir können diese Daten dann mit unserem privaten Schlüssel wieder entschlüsseln.

Wenn wir Ihnen Daten senden, verschlüsseln wir die Daten vorher mit Ihrem öffentlichen Schlüssel. Nur Sie können diese Daten dann wieder mit Ihrem privaten Schlüssel entschlüsseln.

Sie können für die verschlüsselung und Entschlüsselung im Prinzip beliebige Kryptographie-Software verwenden, die dieses asymmetrische Verfahren unterstützt. Wir empfehlen Ihnen hier eine kostenfreie Opensource-Lösung.

Installation der Software

Wir empfehlen Ihnen unter Windows die Verwendung von Gpg4win. Die betreffende Homepage befindet sich hier:

https://www.gpg4win.de/

Wählen Sie auf dieser Seite "Download". Sie können dann etwas an die Ersteller der Software spenden oder Sie wählen 0€ und können den Download direkt starten.

Installieren Sie danach die Software auf Ihrem Windows-PC.



Bitte bei der Installation darauf achten, dass alle Haken gesetzt sind:

Erstellung Ihres Schlüsselpaars

Generieren Sie mit dem nun installierten Programm "Kleopatra" ein Schlüsselpaar für sich. Dieses besteht aus einem geheimen Schlüssel, welcher bei Ihnen auf Ihrem PC verbleibt, und einem öffentlichen Schlüssel. Den öffentlichen Schlüssel benötigen wir, um mit Ihnen verschlüsselte Dateien auszutauschen. Zum Erstellen eines Schlüsselpaares öffnen Sie "Kleopatra".

👩 Kleopatra	the second s	And and a second		
Datei Ansicht Zertifikate Extras Einstellungen	Fenster Hilfe			
Signieren/Verschlüsseln Entschlüsseln/Überprüfen	[프로] [프로] [프 Importieren Beglaub	bigen Auf Server suchen	Ø Notizblock	
Willkommen zu Kleopa Kleopatra ist eine Benutzerob Die meisten Aktionen benötige • Der private Schlüssel • Der öffentliche Schlüs Weitere Informationen finden	tra 3.1.2-gpg4win-3.1.2 erfläche für die Krypto-Anwendung GnuPG. en entweder einen öffentlichen Schlüssel (Zr wird zum Entschlüsseln und Signieren benöt ssel kann von anderen zum Verifizieren Ihrer I Sie bei <u>Wikipedia</u> .	Certifikat) oder Ihren privaten Schlü stigt. Ir Identität oder zum Verschlüsseln	ssel. an Sie verwendet werden.	

Wählen Sie in der Menüleiste Datei -> Neues Schlüsselpaar. Im sich öffnenden Fenster wählen Sie "Persönliches OpenPGP-Schlüsselpaar erstellen". Geben Sie dann Ihren Namen und Ihre Email-Adresse ein und klicken Sie auf "Weiter".

Sie sehen eine Zusammenfassung. Klicken Sie erneut auf "Weiter". Das Programm bittet Sie nun um die Eingabe einer Passphrase (eines Passwortes). Wählen Sie eine starke Passphrase und bestätigen diese. Heben Sie die Passphrase auf. Sie benötigen Sie zum Entschlüsseln von empfangenen Dateien.

Assistent zur Erstellung eines Schlüssel	pinentry-qt
Schlüsselpaar wird erstellt Die Erzeugung eines Schlüssels benötigt sehr dauern	Bitte geben Sie die Passphrase ein, um Ihren Schlüssel zu schützen. Passphrase: Nochmal: Qualität: OK Abbrechen
	<u>W</u> eiter <u>Abbrechen</u>

Nach der Bestätigung haben Sie ein Schlüsselpaar erzeugt. Sie können dieses gerne direkt aus dem folgenden Dialog per Email an uns senden (<u>info@cuviba.com</u>). Falls Sie uns Ihren Schlüssel später senden möchten, können Sie in der Kleopatra-Hauptseite Ihren öffentlichen Schlüssel auch später

"Exportieren" und uns die Schlüsseldatei senden.

ei	Ansicht	Zertifikate	Extras	Einstellungen	Fenster Hill	fe	
			i	<u>x</u>			1
r	** ***		1.1	<u></u>	-		?
6	🕘 Assist	tent zur Erstel	llung ein	es Schlüsselpaar	;		
ſ	Schlü	sselnaar e	rfolare	ich erstellt			
	J	sseipaar e	noigre	ach eistein.	5 1 1 1 1 1	11. 0	6 L 11
	finden S	ie weiter unte	ar wurde n.	erfolgreich erstellt	. Details und Vors	schlage fur weiter	e Schritte
h.	Ergeb	nis					
	Schli	isselpaar erfol erabdruck: 704	greich ers	tellt. CE3D39A7C335D	E969A3D8CB395	1034	
					505/100000555		
	Nächs	te Schritte					
	l.		Sicherhe	itskopie Ihres Schl	üsselpaares erste	ellen	
			Öffent	lichen Schlüssel pe	er E-Mail versend	en	
		Öffen	tlichen So	hlüssel an einen V	erzeichnisdienst i	übermitteln	

Importieren des cuviba-Schlüssels

Unseren öffentlichen Schlüssel erhalten Sie im als Email-Anhang oder laden ihn auf der DQS-Seite unserer Homepage herunter (https://www.cuviba.com/index.php/de/dqs-de). Speichern Sie bitte unsere Schlüssel-Datei an einen Ort Ihrer Wahl auf Ihrem PC.

Öffnen Sie "Kleopatra".

👩 Kleopatra		
Datei Ansicht Zertifikate Extras Einstellungen	Fenster Hilfe	
Signieren/Verschlüsseln Entschlüsseln/Überprüfen	Importieren Emportieren Beglaubigen Auf Server succession	hen Notizblock
Willkommen zu Kleopa Kleopatra ist eine Benutzerot Die meisten Aktionen benötig • Der private Schlüsse • Der offentliche Schlü Weitere Informationen finder	I tra 3.1.2-gpg4win-3.1.2 perfläche für die Krypto-Anwendung <u>GnuPG</u> . en entweder einen öffentlichen Schlüssel (Zertifikat) oder Ihren priva I wird zum Entschlüsseln und Signieren benötigt. ssel kann von anderen zum Verifizieren Ihrer Identität oder zum Versi n Sie bei <u>Wikipedia</u> . in Sie bei <u>Wikipedia</u> .	iten Schlüssel. chlüsseln an Sie verwendet werden.

Klicken Sie bitte auf "Importieren". Jetzt müssen Sie die Datei mit unserem Schlüssel von dem auf Ihrem gespeicherten Ort auswählen. Im nun Folgenden Fenster (Beglaubigung) wählen Sie "Nein".

2	Um ein Zertifikat als gültig (grün) zu markieren muss es beglaubigt werden. Beglaubigen bedeutet das Sie den Fingerabdruck überpüfen. Mögliche Wege dies zu tun sind:
	Die Person anrufen.
	Eine Visitenkarte verwenden.
	Es anhand einer vertrauenswürden Webseite zu prüfen.
	Möchten Sie diesen Prozess jetzt starten?
Dies	se Nachfrage nicht mehr anzeigen

Verschlüsseln von Dateien um diese an uns zu versenden

Mittels Rechtsklick auf die Datei

Es gibt mehrere Wege, Dateien mit Kleopatra zu verschlüsseln. Der einfachste Weg ist, einen Rechtsclick auf die zu verschlüsselnde Datei bzw. Ordner zu machen und aus dem sich öffnenden Kontextmenü "Signieren und verschlüsseln" zu wählen.

Im sich öffnenden Fenster wählen Sie unter "Signieren als" sich selbst und machen ein Häkchen bei "Für andere verschlüsseln". Im Auswahlfeld rechts daneben wählen Sie den importierten cuviba-Schlüssel aus. "Mit Passwort verschlüsseln" lassen Sie bitte nicht angeklickt. Drücken Sie anschließend auf "Verschlüsseln" und geben Sie Ihre Passphrase ein, falls Sie danach gefragt werden. Die verschlüsselte Datei mit der Endung .pgp befindet sich nun im ausgewählten Zielordner (im selben Ordner wie die Ursprungs-Datei, falls Sie den Ordner nicht geändert haben). Schicken Sie die verschlüsselte Datei an uns (info@cuviba.com).

Dateien archivieren und si	gnieren/verschlüsseln - Kleopatra
Dateien signieren, Authentizität sicherstellen (signi	/verschlüsseln eren)
Signieren als:	♥ Marcus Komann <marcus.komann@cuviba.com> (begiaui ♥</marcus.komann@cuviba.com>
Verschlüsseln	
Eür mich verschlüsseln:	Marcus Komann <marcus.komann@cuviba.com> (bec 🔻 🔺</marcus.komann@cuviba.com>
🔽 Für andere verschlüsseln:	🥑 ail.com> beglaubigt (OpenPGP, Erstellt: 16.08.2018) 🔕 😑
	? Bitte geben Sie einen Namen oder eine E-Mail-Ad
Mit Passwort verschlüsseln.	Jeder, dem Sie das Passwort mitteilen, kann die Daten lesen.
Ausgabe	
g	
C:/Beispielordner	
	Signieren / Verschlüsseln Abbrechen

Mittels Kleopatra

Öffnen Sie Kleopatra und wählen Sie den Menüpunkt "Signieren/Verschlüsseln":

Kleopatra itei Ansicht Zertifikate Extras Einstellunge	n Fenster Hilfe				
nieren/Verschlüsseln Dateien verschlüsseln/überprüfen	Importieren Exportieren Beglaubigen	Q Auf Server suchen	Ø Notizblock		
Suchen <alt+q></alt+q>			Alle Zertifikate		-
Name	E-Mail	Benutzerkennun	gen Gültig seit	Gültig bis	D
Erika Musterfrau	erika.musterfrau@klinikum.de	beglaubigt	25.07.2018		Open
Max Mustermann	max.mustermann@cuviba.com	beglaubigt	25.07.2018		Open

Markieren Sie jetzt eine oder mehrere Dateien:

Organisieren 🔻 🛛 Neuer	Ordner		855 - 6] (?
🖈 Favoriten 🏾 🗍	Bibliothek "Dokumente" Daten	Anordnen nach: Ordr	ner 🔻	
Bibliotheken	Name	Änderungsdatum	Тур	
Bilder	name_1.datei	25.07.2018 13:48	DATEI-Da	
Musik	name_2.datei	25.07.2018 13:48	DATEI-Da	
Videos E	name_3.datei	25.07.2018 13:48	DATEI-Da	
	name_4.datei	25.07.2018 13:48	DATEI-Da	Es ist ke
A Heimnetzaruppe	name_5.datei	25.07.2018 13:48	DATEI-Da	Vorschi verfügb
(internet grouppe	name_6.datei	25.07.2018 13:48	DATEI-Da	ranaga
Computer Solution CC:) Compared and CD:) Compared and CD: Compared and CD: Comp				
Datan () DickStat -				

Nun fügen Sie unsere E-Mail-Adresse unter dem Punkt "Für andere verschlüsseln" hinzu, bestätigen den Vorgang und senden uns die verschlüsselte(n) Datei(en)

Authentizität sicherstellen (signi	eren)
Signieren als:	💟 Erika Musterfrau <erika.musterfrau@klinikum.de> (beglaul 🔻</erika.musterfrau@klinikum.de>
/erschlüsseln	
Für mich verschlüsseln:	🕏 Erika Musterfrau <erika.musterfrau@klinikum.de> (beglaul 🔻</erika.musterfrau@klinikum.de>
Für andere verschlüsseln:	🥏 Max Mustermann <max.mustermann@cuviba.com> bec 🔇</max.mustermann@cuviba.com>
	🙎 Bitte geben Sie einen Namen oder eine E-Mail-Adress
Mit Passwort verschlüsseln.	Jeder, dem Sie das Passwort mitteilen, kann die Daten lesen.
Ausoabe	
Jede Datei einzeln verschlüs	sseln / signieren
	4 č.
D:/Documents/Daten	/Datendatei.tar.gpg 🛛 🕢 🛅

Entschlüsseln von Dateien, welche Sie von uns erhalten

Wenn Sie eine Datei von uns erhalten und diese öffnen, müssen Sie ihr Passwort eingeben, sobald Sie hierzu aufgefordert werden:

Ausgabe-Ordner:	D:/Documents	
Operation 1: Ents	chlüsselung: name.datei.gpg	
	pinentry-qt	1
	Sie benötigen eine Passphrase, um den geheimen OpenPGP Schlüssel zu entsperren: "Erika Musterfrau <erika.musterfrau@klinikum.de>" 2048-Bit RSA Schlüssel, ID 01CF11C29ACF3E7A, erzeugt 2018-07-25 (Hauptschlüssel-ID 969A3D8CB3951034). Passphrase:</erika.musterfrau@klinikum.de>	
	OK Abbrechen	

Anschließend öffnet sich dieses Fenster:

🙃 Dateien entschlüsseln/prüfen - Kleopatra	? X
Ausgabe-Ordner: D:/Documents	
Alle Operationen abgeschlossen.	
	100%
Gültige Signatur von <u>max.mustermann@cuviba.com</u>	
Signatur erstellt am Mittwoch, 25. Juli 2018 13:17:31 Mit dem Zertifikat:	
2AB6 AA6D AC86 87AE 36AE 1898 B9AD FA77 C93E F1AA Die Signatur ist gültig und es besteht volles Vertrauen in die Gültigkeit des Zertifikats.	
Alles speichern	Verwerfen

Bitte achten Sie darauf, unter welchem Pfad Sie die Datei speichern bzw. ändern Sie den "Ausgabe-Ordner" (dort wird die Datei bei Ihnen gespeichert). Wenn Sie dann "Alles speichern" drücken, wird die entschlüsselte Datei im Ausgabe-Ordner abgelegt.